



#3

Docket No.: 60188-075

PATENT**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Application of

Makoto FUJIWARA

Serial No.: 09/867,766

Group Art Unit: 2133

Filed: May 31, 2001

Examiner:

For: SEMICONDUCTOR INTEGRATED CIRCUIT AND METHOD OF TESTING
SEMICONDUCTOR INTEGRATED CIRCUIT

**CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT**

Commissioner for Patents
Washington, DC 20231

Sir:

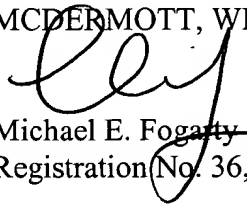
In accordance with the provisions of 35 U.S.C. 119, Applicant hereby claims the priority
of:

Japanese Patent Application No. 2000-161343,
Filed May 31, 2000

cited in the Declaration of the present application. A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY



Michael E. Fogarty
Registration No. 36,139

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 MEF:ykg
Date: October 1, 2001
Facsimile: (202) 756-8087



本 国 特 許 庁 60188-075
JAPAN PATENT OFFICE
May 31, 2001
FUJIWARA

McDermott, Will. & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年 5月31日

出 願 番 号

Application Number:

特願2000-161343

出 願 人

Applicant(s):

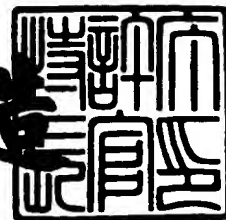
松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 5月18日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3041554

【書類名】 特許願

【整理番号】 5037620067

【提出日】 平成12年 5月31日

【あて先】 特許庁長官 殿

【国際特許分類】 G11C 29/00

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 藤原 睦

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100077931

【弁理士】

【氏名又は名称】 前田 弘

【選任した代理人】

【識別番号】 100094134

【弁理士】

【氏名又は名称】 小山 廣毅

【選任した代理人】

【識別番号】 100110939

【弁理士】

【氏名又は名称】 竹内 宏

【選任した代理人】

【識別番号】 100110940

【弁理士】

【氏名又は名称】 嶋田 高久

【選任した代理人】

【識別番号】 100113262

【弁理士】

【氏名又は名称】 竹内 祐二

【選任した代理人】

【識別番号】 100115059

【弁理士】

【氏名又は名称】 今江 克実

【選任した代理人】

【識別番号】 100115510

【弁理士】

【氏名又は名称】 手島 勝

【選任した代理人】

【識別番号】 100115691

【弁理士】

【氏名又は名称】 藤田 篤史

【手数料の表示】

【予納台帳番号】 014409

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0006010

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 半導体集積回路および半導体集積回路の検査方法

【特許請求の範囲】

【請求項 1】 機密情報データを格納する ROM と、この ROM のテストを行うためのテスト回路とを内蔵した半導体集積回路であって、

前記機密情報データに所定の演算を施して得たチェック用冗長データを、記憶する冗長データ記憶手段を備え、

前記テスト回路は、

前記 ROM から読み出された機密情報データに対し、前記所定の演算に相当する演算を実行するチェック演算回路を有し、このチェック演算回路の演算結果と、前記冗長データ記憶手段に記憶されたチェック用冗長データとの比較を行うことを特徴とする半導体集積回路。

【請求項 2】 請求項 1 記載の半導体集積回路において、

前記冗長データ記憶手段は、前記 ROM であることを特徴とする半導体集積回路。

【請求項 3】 請求項 2 記載の半導体集積回路において、

前記チェック用冗長データは、前記 ROM において、前記機密情報データと異なるアドレスに格納されていることを特徴とする半導体集積回路。

【請求項 4】 請求項 2 記載の半導体集積回路において、

前記チェック用冗長データは、前記 ROM において、前記機密情報データと同一アドレスに格納されていることを特徴とする半導体集積回路。

【請求項 5】 機密情報データを格納する ROM を内蔵した半導体集積回路を検査する方法であって、

前記機密情報データに所定の演算を施して得たチェック用冗長データを、予め、当該半導体集積回路の冗長データ記憶手段に、記憶させておく前処理と、

前記 ROM から機密情報データを読み出し、読み出した機密データに対し、前記所定の演算に相当する演算を実行する処理と、

前記冗長データ記憶手段からチェック用冗長データを読み出し、前記演算処理の結果と、読み出したチェック用冗長データとを比較する処理とを備えたことを特徴とする半導体集積回路の検査方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ROMを内蔵した半導体集積回路について、このROMをテストするための技術に属する。

【0002】

【従来の技術】

図4はROMを内蔵した半導体集積回路のテスト回路の従来の構成を示す図である。図4の構成では、テスト回路として、ROM51の入力側と出力側にセレクタ61、62、63が設けられている。各セレクタ61、62、63は入力Sが“H”のとき、端子Aの入力を選択出力する。

【0003】

ROM51のテストを行うときは、テスト信号TESTとして“H”を与える。これによって、外部端子IN1、IN2への入力データがROM51のアドレス入力ADDおよびリード入力READに供給される。そして、ROM51の出力DOが外部端子OUTから出力される。このように、従来は、ROM51の入出力を外部から直接的に制御可能にすることによって、ROM51のテストを実行していた。

【0004】

【発明が解決しようとする課題】

ところが、従来のように、ROMの入出力を外部から直接的に制御可能にすると、マイクロコード、秘密鍵やパスワードなどのような機密情報データをROMに実装した場合に、その実装した機密情報データが外部から容易に解読されてしまう、という問題が生じる。

【0005】

また、従来のBIST (Built In Self Test) 方式を利用した場合は、データ

の機密性は上述の例よりも高まるものの、機密情報データの内容を変更した場合に、半導体集積回路内に実装するBIST回路自体の構成も変更する必要がある。このため、開発工数やマスク設計費などが大幅に増大してしまう。

【0006】

前記の問題に鑑み、本発明は、ROMを内蔵した半導体集積回路として、ROMに実装したデータの機密性を保ちつつ、ROMのテストを実行可能にすることを課題とする。

【0007】

【課題を解決するための手段】

前記の課題を解決するために、請求項1の発明が講じた解決手段は、機密情報データを格納するROMと、このROMのテストを行うためのテスト回路とを内蔵した半導体集積回路として、前記機密情報データに所定の演算を施して得たチェック用冗長データを記憶する冗長データ記憶手段を備え、前記テスト回路は、前記ROMから読み出された機密情報データに対し、前記所定の演算に相当する演算を実行するチェック演算回路を有し、このチェック演算回路の演算結果と、前記冗長データ記憶手段に記憶されたチェック用冗長データとの比較を行うものである。

【0008】

請求項1の発明によると、ROMから読み出された機密情報データに対し、テスト回路が有するチェック演算回路によって、チェック用冗長データ生成のための所定の演算に相当する演算が実行される。そして、冗長データ記憶手段に記憶されたチェック用冗長データと、チェック演算回路の演算結果とが比較される。これにより、機密情報データが半導体集積回路外部に読み出されることなく、データチェックが実現され、機密情報データの機密性を損なうことなく、ROMのテストを実行することができる。

【0009】

そして、請求項2の発明では、前記請求項1の半導体集積回路における冗長データ記憶手段は、前記ROMであるものとする。

【0010】

さらに、請求項3の発明では、前記請求項2の半導体集積回路におけるチェック用冗長データは、前記ROMにおいて、前記機密情報データと異なるアドレスに格納されているものとする。

【0011】

また、請求項4の発明では、前記請求項2の半導体集積回路におけるチェック用冗長データは、前記ROMにおいて、前記機密情報データと同一アドレスに格納されているものとする。

【0012】

また、請求項5の発明が講じた解決手段は、機密情報データを格納するROMを内蔵した半導体集積回路を検査する方法として、前記機密情報データに所定の演算を施して得たチェック用冗長データを予め当該半導体集積回路の冗長データ記憶手段に記憶させておく前処理と、前記ROMから機密情報データを読み出し、読み出した機密データに対し前記所定の演算に相当する演算を実行する処理と、前記冗長データ記憶手段からチェック用冗長データを読み出し、前記演算処理の結果と読み出したチェック用冗長データとを比較する処理とを備えたものである。

【0013】

【発明の実施の形態】

以下、本発明の一実施形態について、図面を参照して説明する。

【0014】

図1は本発明の一実施形態に係る半導体集積回路の構成を示すブロック図である。図1に示す半導体集積回路は、マイクロコード、秘密鍵やパスワードなどの機密情報データの機密性を損なうことなく、ROM10のテストが実現可能に構成されている。

【0015】

図1において、 $(n+1)$ 個の機密情報データすなわち機密情報データ(0)～(n)が、ROM10の下位アドレスに実装されている。そして、各機密情報データ(0)～(n)について、CRC (Cyclic Redundancy Check: 巡回冗長検査) による冗長コードすなわちチェック用冗長データとしての機密CRCデー

タ、(0)～(n)が生成されており、これらは、冗長データ記憶手段としてのROM10の上位アドレスに実装されている。

【0016】

ROM10のアドレス空間において、機密情報データ(0)～(n)は、最下位アドレスから順に格納されており、機密CRCデータ(0)～(n)は、最上位アドレスから順に格納されている。例えば、ROM10の最下位アドレスに格納された機密情報データ(0)に対する機密CRCデータ(0)は、ROM10の最上位アドレスに格納されている。このようなアドレス配置は、ROM10のコンプリメンタリチェックに適している。

【0017】

また、図1において、セクタ21、22、アドレスデコーダ(ADEC)23、フリップフロップ(FF)24、チェック演算回路(CRC)25および比較回路(COMP)26によって、テスト回路が構成されている。また、論理回路ブロック(LOGIC)30は通常モードで用いられる回路ブロックである。

【0018】

各セクタ21、22は、入力Sが“H”(ハイレベル)になると、入力端子Aの入力を選択出力する。アドレスデコーダ23はテスト時に入力されるアドレス信号をデコードし、チェック演算回路25や比較回路26を制御する。チェック演算回路25はROM10から読み出された機密情報データに対し、機密CRCデータ生成の際の所定の演算に相当する演算を実行する。比較回路26は、チェック演算回路25の出力と、ROM10から読み出された機密CRCデータとを比較する。なお、CLKは、各回路ブロックの同期用クロック信号である。

【0019】

通常動作時は、テスト信号TESTは“L”(ロウレベル)になり、セクタ21、22は入力端子Bの入力を選択する。すなわち、外部端子INA、INBからの入力データがROM10に与えられる。これらの入力データは、半導体集積回路内の別のブロックから供給される。また、ROM10の出力DOは、論理回路ブロック30に供給される。

【0020】

一方、テスト時は、テスト信号TESTは“H”になり、セクタ21, 22は入力端子Aの入力を選択する。すなわち、外部端子IN1, IN2からの入力データが、ROM10のアドレス入力ADDおよびリード入力READに供給される。

【0021】

また、外部端子IN1からの入力データは、アドレスデコーダ23にも入力される。アドレスレコーダ23は、外部端子IN1からの入力データが、機密情報データが格納されているアドレス (address(0)~(n)) を示すときは、出力AOUT1をイネーブル (“H”) にする。出力AOUT1が “H” になると、ROM10の出力DOの先にあるチェック演算回路25が1クロック遅れて動作を開始する。また、外部端子IN1からの入力データが、機密CRCデータが格納されているアドレス (address(n+1)~(2n+1)) を示すときは、アドレスデコーダ23は、出力AOUT2をイネーブル (“H”) にする。出力AOUT2が “H” になると、比較回路26は、チェック演算回路25の演算結果 (IN1) と、ROM10から読み出された機密CRCデータ (IN2) との比較を実行する。そして、比較結果が一致したとき、出力信号RESULTをアサート (“H”) する。

【0022】

図2は図1に示す半導体集積回路のテスト時の動作を示すタイミングチャートである。

【0023】

まず、ROM10のテストを行うモードにするために、テスト信号TESTを “H” にする。次に、外部端子IN1から、ROM10において機密情報データ (0) が格納されたアドレスaddress(0)を示す信号を入力するとともに、外部端子IN2から、ROM10のリード入力READがイネーブルになるように “H” を入力する。すると、次のクロック信号CLKの立ち上がりで、ROM10の出力DOとして機密情報データ (0) が読み出される。

【0024】

また、アドレスデコーダ23は、アドレスaddress(0)を示す信号が入力された

ので、出力AOUT1として“H”を出力する。この信号“H”は、フリップフロップ24で1クロックラッチされた後、チェック演算回路25にイネーブル入力enとして供給される。これにより、チェック演算回路25は、ROM10から出力された機密情報データ(0)に対するCRC演算を開始する。

【0025】

チェック演算回路25がCRC演算を完了する1サイクル前に、外部端子IN1への入力データを、address(0)~(n)以外の値に変更するとともに、外部端子IN2への入力データをネゲート(“L”)にする。すると、アドレスデコーダ23の出力AOUT1もネゲートされ、さらに1サイクル遅れてチェック演算回路25のイネーブル入力enもネゲートされる。これにより、チェック演算回路25の演算結果が出力OUTに保持される。

【0026】

次に、外部端子IN1から、機密情報データ(0)に対応する機密CRCデータ(0)が格納されたアドレスaddress(2n+1)を示す信号を入力するとともに、外部端子IN2から、ROM10のリード信号READがイネーブルになるように“H”を入力する。

【0027】

アドレスデコーダ23は、アドレスaddress(2n+1)を示す信号が入力されたので、出力AOUT1として“L”を入力するとともに、出力AOUT2として“H”を出力する。比較回路26は、チェック演算回路25の出力OUTと、ROM10の出力DOすなわち機密CRCデータ(0)との比較を実行する。そして、この比較の結果、両者が一致しているときは、信号RESULTをアサートし(“H”)、不一致のときは“L”にする。

【0028】

また、出力AOUT2が“H”の間、1サイクル期間は信号COMP enがアサートされ、RESULT信号の出力とともにネゲートされる。また、信号COMP enの立ち下がりによって、チェック演算回路25は初期化される。

【0029】

以上のような動作によって、機密情報データ(0)のテストが完了する。

【 0 0 3 0 】

同様の動作を、アドレスaddress(1)、address(2n)、アドレスaddress(2)、address(2n-1)、…、アドレスaddress(n)、address(n+1)を指定しながら実行し、信号RESULTを外部からモニターする。この結果から、ROM10に、製造上の問題などに起因して異常が生じているか否かを判定することができる。

【 0 0 3 1 】

なお、図1の構成では、機密CRCデータを、機密情報データとは別のアドレスに格納するものとしたが、機密情報データと同一アドレスに格納してもかまわない。例えば図3に示すように、機密情報データの上位側のビット位置に、対応する機密CRCデータをマッピングするようにしてもよい。

【 0 0 3 2 】

また、ここでは、機密CRCデータを、機密情報データが実装されたROM自体に実装するものとしたが、機密情報データが実装されたROMとは別の、半導体集積回路に内蔵されたROMなどの記憶手段に、機密CRCデータを実装してもかまわない。

【 0 0 3 3 】

また、本発明によると、機密情報データの内容を変更する場合には、その変更に応じて、機密CRCデータを変更するだけでよい。したがって、テスト回路の構成の変更は不要であり、このため、開発工数やマスク設計費などを大幅に削減することができる。

【 0 0 3 4 】

また、CRCによる冗長コード以外のデータを、機密情報データのチェックに利用してもかまわない。ただし、この場合は、そのチェック用データを生成するための所定の演算に相当する演算を実行するチェック演算回路を、テスト回路内に設ける必要がある。

【 0 0 3 5 】

なお、本実施形態では、同期ROMを例にとって説明を行ったが、非同期ROMであっても、同様の実施が容易に実現可能である。

【 0 0 3 6 】

【発明の効果】

以上のように本発明によると、機密情報データを格納するROMを内蔵した半導体集積回路において、ROMのテストを、そのROM内部の機密情報データの機密性を損なうことなく、実現することができる。

【図面の簡単な説明】

【図 1】

本発明の一実施形態に係る半導体集積回路の構成を示すブロック図である。

【図 2】

図 1 に示す半導体集積回路のテスト時の動作を示すタイミングチャートである。

【図 3】

ROMにおけるデータ格納の他の例を示す図である。

【図 4】

従来の構成の例を示す図である。

【符号の説明】

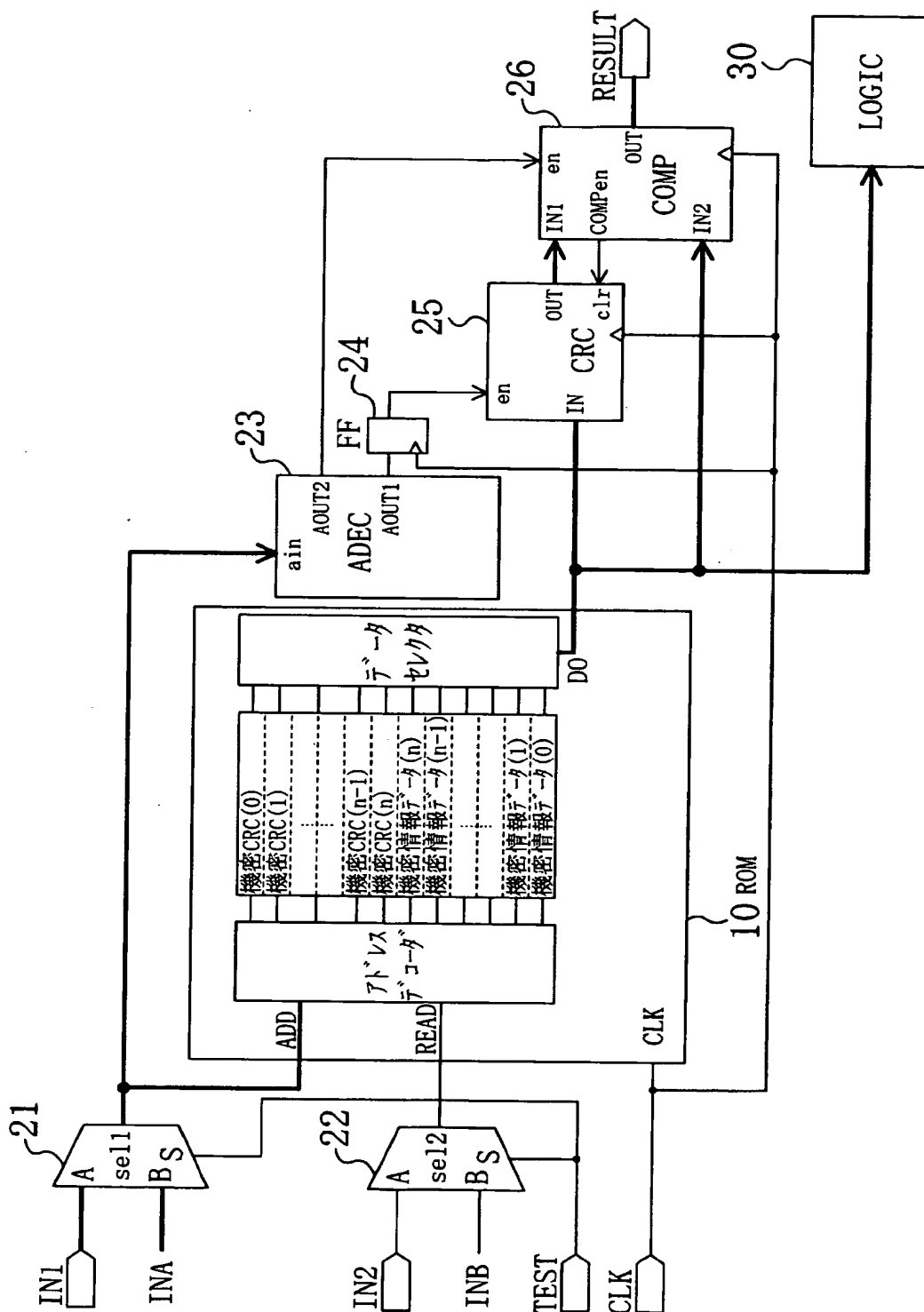
1 0, 1 0 A ROM

2 5 チェック演算回路

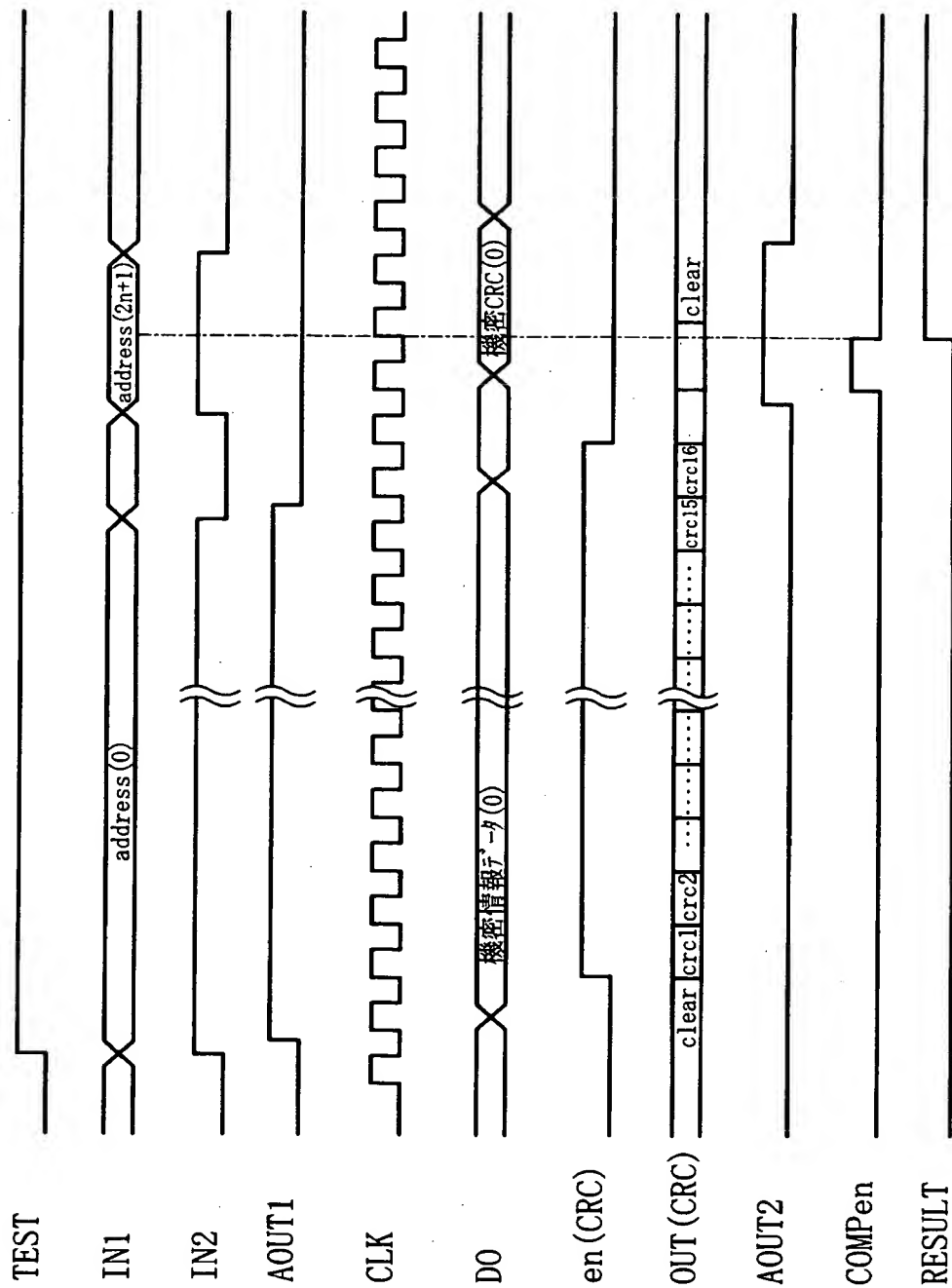
【書類名】

図面

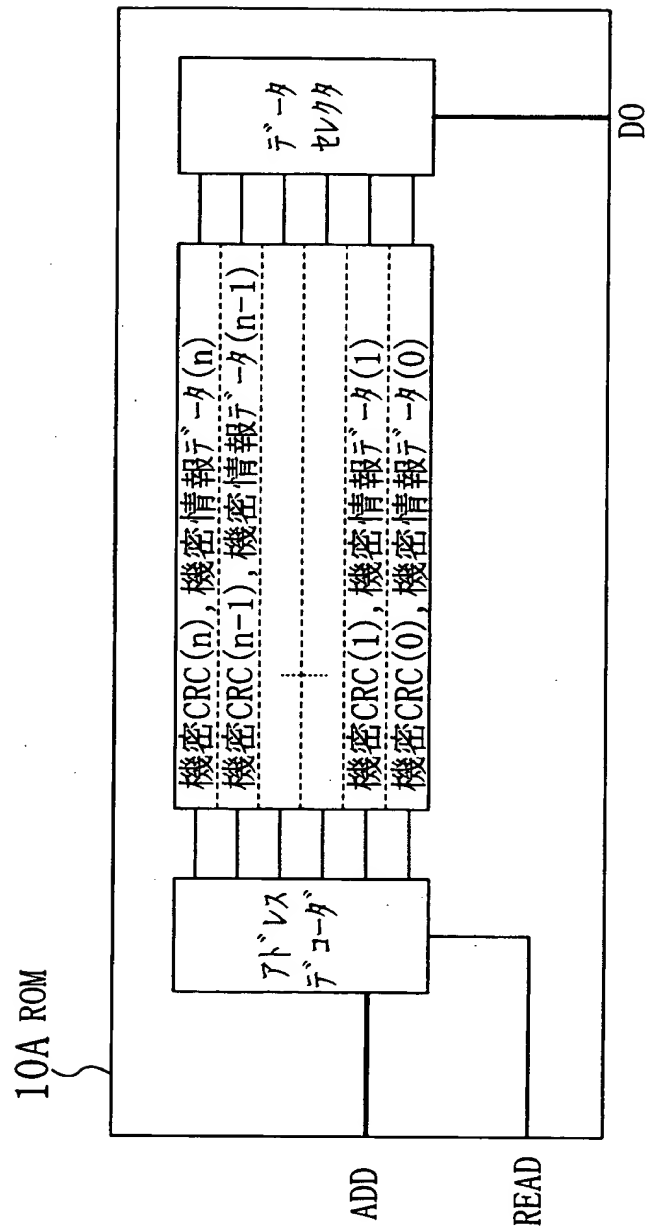
【図 1】



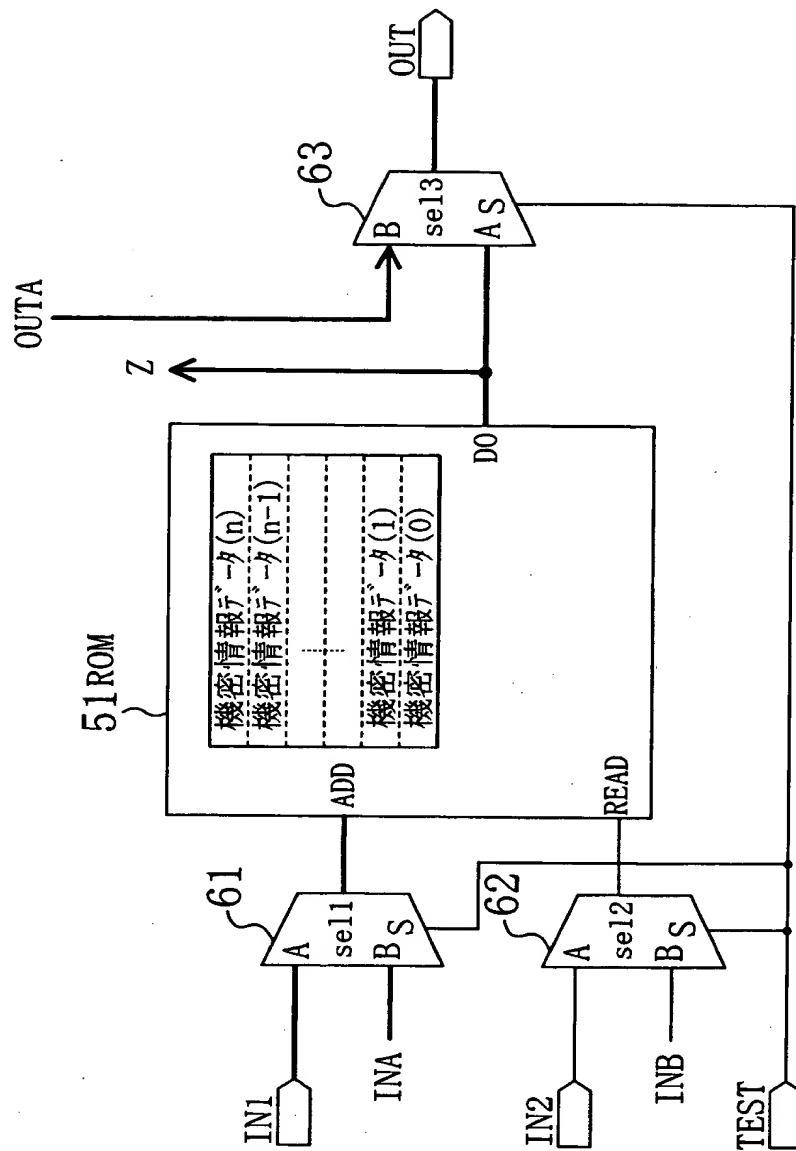
【図 2】



【図 3】



【図 4】



【書類名】 要約書

【要約】

【課題】 ROMを内蔵した半導体集積回路について、ROMに実装したデータの機密性を保ちつつ、ROMのテストを実行可能にする。

【解決手段】 機密情報データを格納するROM10に、データチェック用の機密CRCデータが格納されている。チェック演算回路25は、ROM10から読み出された機密情報データに対し、機密CRCデータ生成のための演算に相当する演算を実行する。比較回路26は、チェック演算回路25の演算結果と、ROM10から読み出された機密CRCデータとの比較を行う。

【選択図】 図1

出 願 人 履 歷 情 報

識別番号 [000005821]

1. 変更年月日	1990年 8月28日
[変更理由]	新規登録
住 所	大阪府門真市大字門真1006番地
氏 名	松下電器産業株式会社